We claim:

1. A method for an enterprise to manage privacy of information, the method comprising:

identifying application information that describes at least one software application used by the enterprise;

storing the application information in a database;

identifying types of information that are contained in or used by the application;

storing the types of information in the database;

determining jurisdiction information that describes the jurisdictions in which the application operates;

storing the jurisdiction information in the database;

identifying the procedures used to protect the privacy of the types of information;

storing procedural information related to the procedures in the database;

automatically determining a compliance rating associated with the application;

storing the compliance rating in the database; and

providing status data from the database, wherein the status data comprises at least the compliance rating.

2. The method according to claim 1, further comprising:

identifying at least one category of functionality performed by the application, where in the procedures used to protect the privacy varies by the category of functionality.

3. The method according to claim 2, wherein the at least one category comprises at least one of: customer services processes; data destruction and disposal procedures; data extraction and modification; development environment processes ; encryption practices; outside service provider practices; related applications and processes; and website practices.

4. The method according to claim 1, wherein the types of information that are contained in or used by the application comprises at least one of: Social Security number; health related information; compensation information; contributions/donation information; employee performance review information; tuition reimbursement information; license and certification information; work experience information; association information; and bio-metric information.

5. The method according to claim 1, further comprising determining a type of functionality conducted with respect to each type of information.

6. The method according to claim 5, wherein the type of functionality comprises at least one of the following: processing; transmitting; collecting; and storing.

7. The method according to claim 6, further comprising determining a information privacy impact rating for the application in response to the types of functionality and types of information.

8. The method according to claim 7 further comprising:

determining if the application has functionality with respect to customer data and employee data; and

wherein the step of determining the information privacy impact rating further comprises determining a customer information privacy impact rating and an employee information privacy impact rating.

9. The method according to claim 1, wherein the step of automatically determining the compliance rating associated with the application is in response to the jurisdiction information.

10. The method according to claim 9, wherein the jurisdiction information is used to determine if the application complies with the laws of the jurisdictions in which the application operates.

11. The method according to claim 1, further comprising:

assigning specific people to fulfill roles with respect to managing the privacy of information, wherein the roles include at least one of data privacy owner and data privacy risk manager.

12. The method according to claim 11, further comprising:

receiving acknowledgements of the acceptances of the assignments from the specific people.

13. The method according to claim 11, further comprising:

assigning alternate people to fulfill the roles.

14. The method according to claim 1, wherein all of the steps of the method are facilitated using a software application, the method further comprising:

generating data input screens for accepting input from a user; and

providing drop down boxes on the data input screens in order to facilitate selection of predefined information.

15. The method according to claim 1, wherein the step of providing status data further comprises:

providing status data on the enterprise level;

providing status data on a line of business level; and

providing status data on a department level.

16. The method according to claim 1, further comprising developing a corrective action plan if the application is not in compliance with the procedures, the corrective action plan containing the steps required to bring the application into compliance.

17. The method according to claim 16, further comprising obtaining an acknowledgement by management of the enterprise of risk associated with the non-compliance of the application.

18. A system for an enterprise to manage privacy of information comprising:

a user interface for interfacing with users of the system;

at least one database server and at least one application server coupled to the user interface; and

at least one database and at least one application respectively coupled to the database server and the application server;

wherein the system is programmed to:

accept application information that describes at least one software application used by the enterprise;

store the application information in a database;

accept types of information that are contained in or used by the application;

store the types of information in the database;

accept jurisdiction information that describes the jurisdictions in which the application operates;

store the jurisdiction information in the database;

accept the procedures used to protect the privacy of the types of information;

store procedural information related to the procedures in the database;

automatically determine a compliance rating associated with the application;

store the compliance rating in the database; and

provide status data from the database, wherein the status data comprises at least the compliance rating.

19. The system according to claim 18, wherein the user interface is used to accept at least one category of functionality performed by the application, where in the procedures used to protect the privacy varies by the category of functionality.

20. The system according to claim 19, wherein the at least one category comprises at least one of: customer services processes; data destruction and disposal procedures; data extraction and modification; development environment processes ; encryption practices; outside service provider practices; related applications and processes; and website practices.

21. The system according to claim 19, wherein the types of information that are contained in or used by the application comprises at least one of: Social Security number; health related information; compensation information; contributions/donation information; employee performance review information; tuition reimbursement information; license and certification information; work experience information; association information; and bio-metric information.

22. The system according to claim 19, wherein the user interface is used to accept a type of functionality conducted with respect to each type of information.

23. The system according to claim 22, wherein the type of functionality comprises at least one of the following: processing; transmitting; collecting; and storing.

24. The system according to claim 22, wherein the system is programmed to determine an information privacy impact rating for the application in response to the types of functionality and types of information.

25. The system according to claim 24, wherein:

the user interface is further used to accept user input indicating if the application has functionality with respect to customer data and employee data; and

the system is further programmed to determine a customer information privacy impact rating and an employee information privacy impact rating.

26. The system according to claim 19, wherein the system is programmed to automatically determine the compliance rating associated with the application is in response to the jurisdiction information.

27. The system according to claim 26, wherein the jurisdiction information is used to determine if the application complies with the laws of the jurisdictions in which the application operates.

28. The system according to claim 19, wherein the database further includes:

assignments of specific people to fulfill roles with respect to managing the privacy of information, wherein the roles include at least one of data privacy owner and data privacy risk manager.

29. The system according to claim 28, wherein the database further includes:

acknowledgements of the acceptances of the assignments from the specific people.

30. The system according to claim 28, wherein the database further includes:

assignments of alternate people to fulfill the roles.

31. The system according to claim 19, wherein user interface further comprises:

data input screens for accepting input from a user; and

drop down boxes on the data input screens in order to facilitate selection of predefined information.